Docket No. 244986US2RD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Akihiko SUGIKAWA

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: WIRELESS COMMUNICATION DEVICE, PORTABLE TERMINAL, COMMUNICATION CONTROL PROGRAM AND COMMUNICATION SYSTEM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120.**

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e):** **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-321348	November 5, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月　５日

出願番号
Application Number: 特願２００２－３２１３４８

[ST. 10/C]: [ＪＰ２００２－３２１３４８]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７４１６

【書類名】　特許願
【整理番号】　13942301
【提出日】　平成14年11月 5日
【あて先】　特許庁長官殿
【国際特許分類】　H04B 7/00
【発明の名称】　近接通信装置、携帯端末、近接通信装置を制御するプログラム、携帯端末を制御するプログラム及び通信システム
【請求項の数】　13
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　杉　川　明　彦
【特許出願人】
【識別番号】　000003078
【住所又は居所】　東京都港区芝浦一丁目１番１号
【氏名又は名称】　株式会社　東　芝
【代理人】
【識別番号】　100075812
【弁理士】
【氏名又は名称】　吉　武　賢　次
【選任した代理人】
【識別番号】　100088889
【弁理士】
【氏名又は名称】　橘　谷　英　俊
【選任した代理人】
【識別番号】　100082991
【弁理士】
【氏名又は名称】　佐　藤　泰　和

【選任した代理人】
　【識別番号】　100096921
　【弁理士】
　【氏名又は名称】　吉　元　弘
【選任した代理人】
　【識別番号】　100103263
　【弁理士】
　【氏名又は名称】　川　崎　康
【手数料の表示】
　【予納台帳番号】　087654
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　近接通信装置、携帯端末、近接通信装置を制御するプログラム、携帯端末を制御するプログラム及び通信システム

【特許請求の範囲】

【請求項１】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置において、

自装置を識別するための自装置情報を取得する自装置情報取得手段と、

自装置が提供するサービス名称と前記自装置情報とを含む第１識別情報を生成する第１識別情報生成手段と、

予め定めた暗号鍵を用いて前記第１識別情報を暗号化して暗号化データを生成する暗号化手段と、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第２識別情報を生成する第２識別情報生成手段と、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第２識別情報を送信する自装置情報送信手段と、を備えることを特徴とする近接通信装置。

【請求項２】

前記第１識別情報生成手段は、前記サービス名称と前記自装置情報とを合わせたデータに対してハッシュ演算を行って得られたハッシュ値を前記第１識別情報とすることを特徴とする請求項１に記載の近接通信装置。

【請求項３】

前記第２識別情報生成手段は、前記サービス名称の後に続けて前記暗号化データを配置し、前記サービス名称の前に、前記サービス名称の長さを示す情報を配置した前記第２識別情報を生成することを特徴とする請求項１または２に記載の近接通信装置。

【請求項４】

前記第２識別情報生成手段は、前記サービス名称の長さを示す情報の前に、高速処理を指示する情報を配置した前記第２識別情報を生成することを特徴とする請求項３に記載の近接通信装置。

【請求項５】

前記近接通信手段は、Bluetoothの仕様で通信を行い、

前記自装置情報は、Bluetoothアドレスであることを特徴とする請求項１及至４のいずれかに記載の近接通信装置。

【請求項６】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末において、

自端末と通信可能な通信装置を探索する探索手段と、

前記探索された通信装置から送信された第１識別情報を取得する識別情報取得手段と、

前記取得された第１識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、

予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、

前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報とを比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、

前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段と、を備えることを特徴とする携帯端末。

【請求項７】

前記比較判定手段により信頼できないと判定された通信装置に利用者が接続しようとした場合に、信頼できないことを示す情報を利用者に提示する情報提示手段を備えることを特徴とする請求項６に記載の携帯端末。

【請求項８】

前記比較判定手段により信頼できないと判定された通信装置の一覧を登録するリスト登録手段を備え、

前記通信制御手段は、前記リスト登録手段に登録されている通信装置との通信を禁止することを特徴とする請求項７に記載の携帯端末。

【請求項９】

前記情報抽出手段で抽出されたサービス名称及び装置識別名称をあわせたデー

タに対してハッシュ演算を行ってハッシュ値を生成するハッシュ演算手段を備え、

前記比較判定手段は、前記復号されたデータと前記生成されたハッシュ値とを比較することを特徴とする請求項６及至８のいずれかに記載の携帯端末。

【請求項１０】

前記近接通信手段は、Bluetoothの仕様で通信を行い、

前記自装置情報は、Bluetoothアドレスであることを特徴とする請求項６及至９のいずれかに記載の携帯端末。

【請求項１１】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置を制御するコンピュータ読み取り可能なプログラムにおいて、

自装置を識別するための自装置情報を取得するステップと、

自装置が提供するサービス名称と前記自装置情報とを含む第１識別情報を生成するステップと、

予め定めた暗号鍵を用いて前記第１識別情報を暗号化して暗号化データを生成するステップと、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第２識別情報を生成するステップと、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第２識別情報を送信するステップと、を備えることを特徴とする近接通信装置を制御するプログラム。

【請求項１２】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末を制御するコンピュータ読み取り可能なプログラムにおいて、

自端末と通信可能な通信装置を探索するステップと、

前記探索された通信装置から送信された第１識別情報を取得するステップと、

前記取得された第１識別情報から、サービス名称、自装置情報及び暗号化デー

タを抽出するステップと、

予め定めた解読鍵を用いて、前記暗号化データを復号するステップと、

前記復号されたデータと、前抽出されたサービス名称及び自装置情報とを比較し、前記探索された通信装置が信頼できるか否かを判定するステップと、

信頼できないと判定された通信装置との通信を禁止するステップと、を備えることを特徴とする携帯端末を制御するプログラム。

【請求項１３】

携帯端末と、所定の範囲内に位置する前記携帯端末との間で通信を行うことが可能な近接通信手段と、を備えた通信システムにおいて、

前記携帯端末は、

自端末と通信可能な通信装置を探索する探索手段と、

前記探索された通信装置から送信された第１識別情報を取得する識別情報取得手段と、

前記取得された第１識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、

予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、

前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報とを比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、

前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段と、を有し、

前記近接通信装置は、

自装置を識別するための自装置情報を取得する自装置情報取得手段と、

自装置が提供するサービス名称と前記自装置情報とを含む第１識別情報を生成する第１識別情報生成手段と、

予め定めた暗号鍵を用いて前記第１識別情報を暗号化して暗号化データを生成する暗号化手段と、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第２識別情報を生成する第２識別情報生成手段と、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第２識別情報を送信する自装置情報送信手段と、を有することを特徴とする通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、Bluetoothなどの比較的狭い範囲で通信を行う近接通信装置と、この種の近接通信装置と通信を行う携帯端末とに関する。

【０００２】

【従来の技術】

最近、伝送距離が１０ｍ程度の近距離無線通信方式が注目を集めている。従来の無線ＬＡＮの有効な伝送距離範囲が１００ｍ以上であるのに対し、近距離無線通信方式は、伝送範囲が狭い分、使用する電力が少ないので、携帯電話やＰＤＡ等の携帯型情報処理装置（以下、簡単に携帯端末と呼ぶ）などのバッテリーに制限がある情報処理装置に適している。

【０００３】

Bluetooth（登録商標）は、このような近距離無線通信方式の１つであり、近年、このBluetooth通信機能を備えた携帯端末が普及し始めている（非特許文献１参照）。

【０００４】

Bluetoothは、デバイスの単価が安くて装置の小型化が可能なため、Bluetooth通信機能を備えた装置が今後いたるところに普及すると予想される。Bluetoothの普及により、任意の場所で、各場所に応じたサービスや情報を提供できるようになる。

【０００５】

例えば、コンビニエンスストア、スーパ及び小売店などでは、電子クーポンサービス、電子ポイントサービス、電子決済、レシート及び領収書発行などの購買者向けのサービスを行うことができる。また、電子チケットによるゲート開閉の制御、自動販売機での決済や割引サービス、駐車場、ガソリンスタンド及びドライブスルーでの料金支払いなどへの応用が期待されている。この他、インターネ

ットへのアクセス、情報配信及び位置情報の提供なども可能になる。特に、人が多く集まるような駅や待ち合わせのスポットには、Bluetooth通信機能を備えた数多くの装置が設置されることが予想される。

【０００６】

以下、Bluetooth通信機能を備えた携帯端末（以下、簡単にBluetooth端末と呼ぶ）と、Bluetooth通信機能を備えて各種サービスを提供する情報処理装置（以下、簡単にBluetooth装置と呼ぶ）との間で、Bluetoothによる接続を確立し、当該Bluetooth端末を所持するユーザにBluetooth装置がサービスを提供する場合を例にとって、従来技術を説明する。

【０００７】

まず、Bluetooth端末が任意の場所で任意の相手からサービスを受けるための手順を説明する。図８はこの手順を示すフローチャートである。まず、サービスを受けるためのアプリケーションを起動する（ステップＳ１）。次に、Bluetooth端末は、インクワイアリを行って周囲の通信可能な端末の発見を試みる（ステップＳ３）。

【０００８】

次に、Bluetooth端末は、発見した端末のリモートネームを取得する（ステップＳ４）。次に、一定時間経過後、インクワイアリが完了すると、Bluetooth端末は、インクワイアリで発見した装置のリモートネームの一覧を利用者に提示する（ステップＳ５）。

【０００９】

次に、Bluetooth端末は、利用者が選択したBluetooth装置に対してACL接続要求を行う（ステップＳ６）。そして、ACL接続完了後、Bluetooth端末は、サービス情報取得コマンドを送信する（ステップＳ７）。

【００１０】

次に、Bluetooth端末は、サービス情報を取得し、アプリケーションが利用するプロファイルをサポートしているか検査する（ステップＳ８）。プロファイルをサポートしている場合は、Bluetooth端末は、そのプロファイルに関する接続情報を取得する（ステップＳ９）。

【００１１】

Bluetooth端末は、取得した情報を用いてそのプロファイルに対して接続要求を行う（ステップＳ１０）。プロファイルの接続完了後、Bluetooth端末は、アプリケーションレベルでサーバ認証を行う（ステップＳ１１）。

【００１２】

以上の手順により、利用者は、Bluetooth端末を使用して所望のサービスを受けることが可能となる。

【００１３】

【特許文献１】

特開２００２－１５２１９６公報　（←ハッシュデータ比較によるプログラムID認証）

【非特許文献１】

Member Web Site、“Specifications”他、［online］、The Bluetooth SIG, Inc.、［平成１４年１０月２９日検索］、インターネット＜URL：http://www.bluetooth.org＞

【００１４】

【発明が解決しようとする課題】

ここで、Bluetoothを使用したサービスや情報提供装置が普及し、公衆の集まる駅やスポットにBluetooth装置が多数配置された状況での使用を想定して説明する。特に人の多く集まるような場所では、有益な情報ばかりでなく、多くの人には無益の情報（ローン、アダルト情報、ギャンブル等）も多数配信されることが容易に想像できる。

【００１５】

このような状況で、サービスや情報を取得しようとして、Bluetooth端末から通信可能なBluetooth装置の発見を試みると、有益無益にかかわらず多くのBluetooth装置が発見されることとなる。

【００１６】

現状では、インクワイアリで取得できる情報に含まれるBluetooth装置の種類に関する情報を記したCOD(Class of Device)を用いれば、所望のサービスを提供

するBluetooth装置のみを絞り込むことができる。

【００１７】

しかし、CODは、装置の種類であってサービスそのものを識別しているのではない。例えば、CODに情報配信装置のカテゴリーがあったとしても、それが、どのような情報を配信する装置かをCODのみでは識別できず、リモートネームで相手装置の名前を取得して初めてわかることである。

【００１８】

ところが、リモートネームは容易に設定できるため、その装置が本当にそのサービスや情報を提供しているかは、サービス提供を行うプロファイル、例えば、ＦＴＰプロファイルの接続を行い、実際に情報を取得しなければわからない。

【００１９】

特定の情報を取得するための専用のアプリケーションを使用するのであれば、例えば、居酒屋情報が欲しい場合は、そのアプリケーションにあらかじめ居酒屋情報提供装置に共通な鍵を持たせておき、Bluetoothのリンク認証機構、あるいは、OBEXの相手認証機能を用いることにより、偽者の装置に接続することを防ぐことができる。

【００２０】

ただし、Bluetoothリンク認証やOBEXの認証も、利用者がその装置に接続を行うまで、正しい装置かどうか確認できないため、無益な情報を提供する装置が多数存在すると、利用者が本来必要とするサービスや情報取得にかかる時間や手間が増えてしまう。

【００２１】

また、リモートネームに利用者の興味をひく宣伝文だけを埋め込んでおいた場合、利用者が通信可能な装置を探索したときに、その宣伝文句を目にすることになり、利用者が希望する端末の選択を阻害することとなる。

【００２２】

リモートネームは容易に設定できるため、その装置が利用者の所望のサービスや情報を本当にサポートしているかは、接続してみて実際に確認しなければならず、利用者に余分な時間や労力をかけることとなる。

【００２３】

また、リモートネームに宣伝文句が設定された装置が存在すると、利用者が接続を希望する装置の選択を大きく阻害してしまう。

【００２４】

本発明は、このような点に鑑みてなされたものであり、その目的は、信頼できるサービスを提供する通信装置に簡易かつ迅速かつ正しく接続可能な近接通信装置、携帯端末、近接通信装置を制御するプログラム及び携帯端末を制御するプログラムを提供することにある。

【００２５】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置において、自装置を識別するための自装置情報を取得する自装置情報取得手段と、自装置が提供するサービス名称と前記自装置情報とを含む第１識別情報を生成する第１識別情報生成手段と、予め定めた暗号鍵を用いて前記第１識別情報を暗号化して暗号化データを生成する暗号化手段と、前記サービス名称、前記自装置情報及び前記暗号化データを含む第２識別情報を生成する第２識別情報生成手段と、前記自装置情報の送信要求を行った他の通信装置に対して、前記第２識別情報を送信する自装置情報送信手段と、を備える。

【００２６】

また、所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末において、自端末と通信可能な通信装置を探索する探索手段と、前記探索された通信装置から送信された第１識別情報を取得する識別情報取得手段と、前記取得された第１識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報とを比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段

と、を備える。

【００２７】

【発明の実施の形態】

以下、本発明に係る近接通信装置、携帯端末、近接通信装置を制御するプログラム及び携帯端末を制御するプログラムについて図面を参照しながら具体的に説明する。以下では主に、Bluetooth端末とBluetooth装置との間でBluetoothによる接続を確立し、当該Bluetooth端末を所持するユーザにBluetooth装置が情報を提供する場合を例にとって説明する。

【００２８】

図１は本発明に係る情報提供装置の一実施形態であるBluetooth装置１０の内部構成を示す図である。Bluetooth装置１０は、バス１に接続されたCPU２、メモリ３、ROM４、記憶装置５、RS-232Cコントローラ６及び有線／無線通信部７と、RS-232Cコントローラ６に接続されたBluetooth送受信部（以下、BT送受信部）８とを有する。

【００２９】

BT送受信部８は、Bluetooth携帯端末１１との間で、Bluetoothの仕様で通信を行う。Bluetooth携帯端末１１に提供する各種の情報は、記憶装置５に格納しておいてもよいし、有線／無線通信部７を介してインターネット９上のサーバに格納しておき、このサーバにアクセスして、Bluetooth携帯端末１１から要求のあった情報を取得してもよい。

【００３０】

記憶装置５の具体的形態は特に問わないが、ハードディスク、DVD-RAM、DVD-ROM及び半導体ディスクなどが考えられる。有線／無線通信部７は、有線及び無線のどちらで通信を行ってもよい。有線で通信を行う場合、イーサネット（登録商標）とIPプロトコル、あるいは、電話線、PPP及びIPなどの組み合わせが考えられる。無線で通信を行う場合、無線インターネットを使用するか、携帯電話やPHSのパケット通信を使用してもよい。

【００３１】

BT送受信部８は、単にBluetooth送受信用モジュールのみの構成、あるいは、B

T送受信部８に別途CPUやメモリを搭載し、上位のプロトコル、たとえば、L2CAPやRFCOMMなどの処理を行う構成のどちらでもよい。

【００３２】

Bluetooth送受信用モジュールのみの構成の場合、仕様書で定義されたHCI(Host Controler Interface)コマンドを送信し、その結果をイベントとして受信する。Bluetoothプロトコルは、利用者へのサービスや情報提供を行うアプリケーションプログラムと共に、CPU２によりメモリ３にロードされ実行される。その他、ＯＳ、ドライバ、アプリケーションは、メモリ３に記憶されている。上位のプロトコルの処理を行う構成の場合、実装に依存したコマンドやイベントを使用して、BT送受信部８の制御とデータの送受信を実現する。

なお、BT送受信部８は、必ずしもRS-232Cを介してホストに接続する必要はなく、例えば、ホストの内部バスに直接接続してもよいし、ＵＳＢ（Universal Serial Bus）を介して、接続してもよい。

【００３３】

図２は、Bluetooth携帯端末１１の内部構成の一例を示すブロック図である。図２のBluetooth携帯端末１１は、バス１２に接続されたCPU１３、メモリ１４、ROM１５、A/D変換器１６、D/A変換器１７、偏心モータ１８、通信部１９、表示部２０、キー入力部２１、EEPROM２２、選択指示部２３及びBT送受信部２４を有する。A/D変換器１６にはマイク２５が接続され、D/A変換器１７にはスピーカ２６が接続されている。通信部１９は、有線または無線により基地局２７と通信を行う。

【００３４】

BT送受信部２４は、例えばBluetooth装置１０との間で無線通信路を確立し、Bluetooth装置１０あるいはインターネット上のサーバに対して情報送信要求コマンドを送信したり、このコマンドに対応する情報を取得したりする。

【００３５】

BT送受信部２４は、Bluetooth装置１０内のBT送受信部８と同様の構成でもよいし、異なる構成でもよい。

【００３６】

Bluetooth携帯端末１１の音声通話機能は、従来の携帯電話と同様であり、例えば、通信部１９は、基地局２７との間で位置登録、発呼・着呼時の呼制御を行ってデータの送受信を行い、通信が終了すると切断の呼制御を行い、通信中はハンドオーバ等を行う。

【００３７】

通信部１９は、基地局２７からの接続要求を受信すると、スピーカ２６から呼び出し音を出力する。あるいは、偏芯モータ１８を駆動させて、Bluetooth携帯端末１１の筐体を振動させてユーザの注意を喚起する。ユーザの接続了解指示を受信すると、キャリアは２地点間の回線接続を行い、通信が開始される。

【００３８】

Bluetooth携帯端末１１は、通信時には、マイク２５から入力された音声をＡ／Ｄ変換部１６でアナログ信号からデジタル信号に変換し、CPU１３の制御の下、デジタルデータの圧縮処理を行い、通信部１９を通じて近接の基地局２７に送信する。また、通信部１９で受信された信号は、CPU１３の制御の下、伸張処理等を施されて元の信号に戻され、Ｄ／Ａ変換部１７でデジタル信号からアナログ信号に変換され、スピーカ２６から出力される。

【００３９】

CPU１３、メモリ１４、ROM１５、表示部２０、キー入力部２１、EEPROM２２及び選択指示部２３は、主に通話以外の目的、すなわち各種情報処理を行う等のために設けられる。例えば、CPU１３は、制御プログラムやアプリケーションプログラムの実行を行う。メモリ１４は一時的な変数や作業データなどを格納する。ROM１５はプログラムや辞書データを記憶する。表示部２０はメニューやデータなどを表示する。キー入力部２１は、電話番号、数字及び文字などを入力する。EEPROM２２は個人登録情報などを保存する。選択指示部２３は、メニュー等の選択を行う。

【００４０】

BT送受信部２４から取得した情報は、そのまま、あるいは表示用のフォーマットに変換されて、表示部２０に表示される。

【００４１】

図３はBluetooth携帯端末１１の情報取得方法を示すフローチャートである。まず、通信可能な相手装置を発見するインクワイアリを実行する（ステップＳ２１）。インクワイアリを行う側（この場合、Bluetooth携帯端末１１）はマスタ、インクワイアリスキャンを行う側（この場合、Bluetooth装置１０）はスレーブと呼ばれる。インクワイアリスキャン状態に設定されたBluetooth装置１０のみがBluetooth携帯端末１１からのインクワイアリに返答する。

【００４２】

Bluetooth携帯端末１１は、インクワイアリを行うために、IQパケットを通常１０秒間周囲にブロードキャストする（ステップＳ２２）。IQパケットにはIAC(Inquiry Access Code)が含まれており、このコードを使用してすべての、あるいは、特定のデバイス（Bluetooth装置１０）の発見を行う。自装置に関連するIACを含むIQパケットを受信したBluetooth装置１０は、ランダムに決められた時間待機後、再度IQパケットを受信すると、自装置のBluetoothアドレス、クロック、デバイスクラスなどの属性をBluetooth携帯端末１１に返信する。

【００４３】

Bluetooth携帯端末１１は、各Bluetooth装置１０からの返信を受け取ると（ステップＳ２３）、FHSパケットの含まれたBluetooth装置１０のBluetoothアドレス、クロック及びCODを取得し（ステップＳ２４）、あらかじめCODが指定されているのであれば、指定されたCODを持つBluetoothアドレスのみ一時的にメモリ１４のリストに記録する（ステップＳ２５，Ｓ２６）。

【００４４】

決められた時間インクワイアリを行うと、インクワイアリ完了イベントを受信する。このイベントを受信すると、Bluetooth装置１０が見つかった否かを判定し（ステップＳ２７）、見つからなかった場合はその旨を表示する(ステップＳ２８)。見つかった場合は、メモリ１４のリストに先ほど記録したBluetoothアドレスを持つBluetooth装置１０に対して、利用者の装置識別に役立つリモートネーム取得コマンドを送信する。このとき、先ほど取得したBluetooth装置１０のクロック情報を用いると、取得時間を短縮することができる。

【００４５】

リストに記録したBluetooth装置１０からリモートネームの要求に対する返信を受信すると（ステップＳ２９）、その結果を先ほど取得したBluetoothアドレス、クロック、デバイスクラスと合わせて記録しておき（ステップＳ３０）、その結果を表示部２０に提示する（ステップＳ３１，Ｓ３２）。

【００４６】

利用者はその中から所望の装置を選択し、対応するBluetoothアドレスを取得して、その装置に対して接続要求を行う（ステップＳ３３，Ｓ３４）。セキュリティを有している場合は、認証用のリンクキーの入力、あるいは、リンクキーを作成するためのPINコードを入力が求められる。適切な値を設定すると、マスターとスレーブ間でデータ通信用のリンクが確立する（ステップＳ３５）。リンク確立後、関連するプロファイル間での接続が行われて通信が可能となる。リンクが確立しなければ接続エラー表示を行う（ステップＳ３６）。

【００４７】

リンクが確立すると、上位プロトコルで接続し（ステップＳ３７）、情報の取得要求を送信すると（ステップＳ３８）、情報を取得して（ステップＳ３９）、情報を表示する（ステップＳ４０）。

【００４８】

Bluetooth装置１０が自装置内の記憶装置５に保存された情報を提供する場合には、オブジェクト・プッシュ・プロファイルやファイル転送プロファイルが用いられ、L2CAP、RFCOMM、FTPプロトコルが使用される。有線／無線通信部７を用いてインターネット上の情報にアクセスする場合は、ダイアルアップ・プロファイルやPANプロファイルが用いられ、ダイアルアップ・プロファイルにはL2CAP、RFCOMM、PPP、IP、HTTPプロトコルが使用され、PNAプロファイルにはL2CAP、イーサエミュレーション、IP及びHTTPプロトコルが使用される。FTPによりBluetooth装置１０から取得した情報や、HTTPによりインターネット上のサーバから取得した情報は、そのまま、あるいは表示用に整形して表示される。

【００４９】

次に、情報提供を行うBluetooth装置１０の処理手順を説明する。まず、Bluetooth装置１０の製造組立て時に接続情報を自装置内部に記録しておく実施形態に

ついて説明する。

【００５０】

図４はサービス提供を行う前のBluetooth装置１０の準備作業を示すフローチャートである。仮に、Bluetooth装置１０の６バイトであるBTアドレスを「012345ABCDEF」の１２文字で表現し、Bluetooth装置１０が提供するサービスあるいは情報を表すサービス名称を「浜松町駅周辺案内情報」の１０文字で表現するものとする（ステップＳ５１）。前者をBTアドレス文字、後者をサービス名称文字と定義する。

【００５１】

これら２つの文字をあわせた２２文字のデータは、１文字２バイトデータで表現されるため、全体で４４バイト、３５２ビットのサイズになる。これをBTアドレス付きサービス名称文字と定義する（ステップＳ５２）。

【００５２】

この３５２ビットのデータに対してハッシュ演算を行い、１２８ビットのハッシュ値を得る（ステップＳ５３）。計算した１２８ビットのハッシュ値に対して、あらかじめ準備された秘密鍵を用いて１２８ビットの暗号化データを求める（ステップＳ５４）。ハッシュ値の計算にはＭＤ５、暗号化にはラインデール方式が利用できる。これらは１例であって１２８ビットのデータが扱える他の方式でも同等の効果を得られる。暗号鍵は１２８ビット以外のものも使用可能であり、鍵長により、計算時間とセキュリティ強度のトレードオフとなる。

【００５３】

暗号化された１６バイト１２８ビットのデータを３２文字のデータに変換する、例えば、「0A4F5G･･･････59EF」とする。BTアドレス付きサービス名称文字と変換されたデータを合わせたものを認証文字と定義する（ステップＳ５５）。この例では、認証文字は、「浜松町駅周辺案内情報012345ABCDEF0A4F5G･･･････59EF」となる。

【００５４】

次に、サービス名称の文字の長さを「010」の３文字で表現し、これをサービス名称長さ文字と定義する（ステップＳ５６）。３文字のサービス名称長さ文字

、１０文字のサービス名称文字、３２文字の認証文字をあわせた４５文字を認証付きサービス名称文字と定義する（ステップＳ５７）。この例では、認証付きサービス名称文字は、「010浜松町駅周辺案内情報012345ABCDEF0A4F5G･･･････59EF」となる。

【００５５】

また、処理を高速化するために頭に識別文字、例えば、２文字の「!!」を挿入したものをBluetooth装置１０の装置識別情報と定義する（ステップＳ５８）。この例では「!!010浜松町駅周辺案内情報012345ABCDEF0A4F5G･･･････59EF」となる。

【００５６】

なお、上述した識別文字中の各文字の配置方法は一例であり、他の配置方法でも同等の効果が得られる。また、バイナリー文字データの変換を単純に２バイトコードで処理しているが、UUENCODEと呼ばれる変換方式では、変換後の文字データのサイズをもとの３分の４程度に抑えることができる。

【００５７】

上記処理を秘密鍵管理で安全に行うには、セキュリティ性の高い装置でBluetooth装置１０ごとにBluetooth装置１０の装置識別情報を計算し、作成されたBluetooth装置１０の装置識別情報を、各Bluetooth装置１０の記憶装置５に記録しておく（ステップＳ５９）。また、秘密鍵とCODの値を情報取得JAVA（登録商標）アプリケーションの初期データとして作成し（ステップＳ６０）、JAVAプログラムとあわせてインターネット上のサーバを通じて利用者に配布する（ステップＳ６１）。情報取得を望む利用者は、公衆網を通じて特定のサーバにアクセスを行い（ステップＳ６２）、JAVAアプリケーションをダウンロードし、自端末に保存しておき、情報を取得する時にJAVAアプリケーションを使用する（ステップＳ６３）。

【００５８】

秘密鍵はJAVAプログラムとともにあわせて配布してもよい、あるいは、あとで説明するがBluetooth装置１０で秘密鍵をセキュアに管理できる場合は、定期的にJAVAアプリケーションが専用のサーバに取得することにより更新することも可

能である。

【００５９】

次に、Bluetooth装置１０のサービス提供時の処理を説明する。図５はBluetooth装置１０のサービス提供時の処理手順を示すフローチャートである。情報提供を行うBluetooth装置１０の電源投入時に、必要なプログラムが記憶装置５からメモリ３に読み込まれ、情報提供を実現するアプリケーションが動作を開始する（ステップＳ７１）。アプリケーションは、利用者の所持するBluetooth携帯端末１１との接続を実現するためにBT送受信部８の制御とBluetoothプロトコルを実現するスタックを実行する（ステップＳ７２）。

【００６０】

アプリケーションは、まずBT送受信部８に対してリセットコマンドを送信する（ステップＳ７３）。次に、アプリケーションは、Bluetooth装置１０の装置識別情報を、他装置からリモートネーム取得コマンドで取得可能な自装置のローカルネームに設定する（ステップＳ７４）。次に、アプリケーションは、CODデバイスをオブジェクト送信系、あるいは、インフォメーション系として設定する（ステップＳ７５）。

【００６１】

その後、インクワイアリスキャンとページスキャンを有効とすることで（ステップＳ７６）、Bluetooth携帯端末１１からの接続待ち状態となる（ステップＳ７７）。Bluetooth携帯端末１１が接続すると（ステップＳ７８）、インクワイアリスキャンとページスキャンを無効にし（ステップＳ７９）、接続したBluetooth携帯端末１１に対してサービスを提供し（ステップＳ８０）、サービス提供が完了すると、接続を切断する（ステップＳ８１）。

【００６２】

次に、Bluetooth携帯端末１１の動作を説明する。図６はBluetooth携帯端末１１の処理手順を示すフローチャートである。情報取得を目的とする利用者は、専用のJAVAアプリケーションの起動を指示し、Bluetooth装置１０の探索を指示する（ステップＳ９１）。JAVAアプリケーションは、BT送受信部２４に対してインクワイアリコマンド送信を要求する。この探索は、所定時間（例えば、１０秒間

）行われる（ステップＳ９２）。

【００６３】

BT送受信部２４は、発見したBluetooth装置１０のアドレス、CODをJAVAアプリケーションにイベントとして通知する（ステップＳ９３）。JAVAアプリケーションは、通知により特定の関数をコールし、CODの検査を行う（ステップＳ９４）。BT送受信部２４は、あらかじめ定めたCODとの比較を行い（ステップＳ９５）、一致した場合のみ、そのBluetooth装置１０のBluetoothアドレスを検査対象リストに加える（ステップＳ９６）。

【００６４】

BT送受信部２４は、一定期間経過するとインクワイアリを中止し、インクワイアリ完了イベントをアプリケーションに通知する。アプリケーションは、インクワイアリ完了イベントを受信すると、検査対象リストに記録されているBluetooth装置１０が存在するか否かを判定し（ステップＳ９７）、存在しなければ、端末なしを表示する（ステップＳ９８）。

【００６５】

検査対象リストに記録されているBluetooth装置１０が存在すれば、そのリストに記録した各装置１０に対して順番にリモートネーム取得コマンドを送信するようBT送受信部２４に指示し（ステップＳ９９）、各Bluetooth装置１０が正しい装置か否かを検証した結果をフラグとして記録する（ステップＳ１００，Ｓ１０１）。リモートネームの取得と検証をリストに記録した端末の数だけ繰り返し（ステップＳ１０２）、各装置が信頼できるかどうか個別に判定を行う。

【００６６】

すべての検査対象のBluetooth装置が信頼できるかどうかを判定するフラグを検査し、信頼できる装置の場合は、そのサービス名称をサービス提供装置の候補として画面に表示する（ステップＳ１０３）。信頼できない装置の場合は、画面に表示しない、あるいは、信頼できる装置とは区別できる形式で表示する。信頼できない装置を表示する／しないは、利用者が別途設定できるようにする。また区別する方法としては、異なる色で表示する、イタリックの書体を用いる、マークをつけるなどが考えられる。

【００６７】

また、利用者が信頼できないBluetooth装置１０への接続要求を行った場合は、利用者に検証できない装置であることを提示して、接続の確認を行う（ステップＳ１０４）。

【００６８】

次に、図６のステップＳ１００の検証の手順を図７のフローチャートを用いて詳しく説明する。最初に検証用のデータの取得方法、次に取得したデータを持いた検証方法を説明する。

【００６９】

BT送受信部２４は、通信相手のBluetooth装置１０のBluetoothアドレスを読み出して（ステップＳ１１１）、リモートネームを取得すると（ステップＳ１１２）、JAVAアプリケーションに通知する。JAVAアプリケーションは、取得したリモートネームのデータを検査する。

【００７０】

JAVAアプリケーションは、最初に取得したリモートネームの最初の数文字が識別文字か否かを判定する（ステップＳ１１３）。この場合は、「!!」である。識別文字と一致しない場合は、検査対象のBluetooth装置１０のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ１４に記録し、次のBluetooth装置１０のリモートネームを取得する。

【００７１】

識別文字と一致した場合は、３文字目（バイナリデータで計算すると６バイト）から３文字（バイナリデータでは６バイト）「010」を切り出し、そのデータをサービス名称長さ文字であると解釈し、文字数字データ変換を行いサービス名称の長さを得る（ステップＳ１１４）。

【００７２】

変換時にエラーが生じた場合は、検査対象のBluetooth装置１０のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ１４に記録し、次のBluetooth装置１０のリモートネームを取得する。

【００７３】

数字に変換できた場合は、取得した長さの分６文字目から、この例では１０文字分の文字「浜松町駅周辺案内情報」をサービス名として取得する（ステップＳ１１５）。６文字＋サービス名称文字の長さ＋１、この場合１６文字目から１２文字をBTアドレス文字として取得し、６バイトのBluetoothアドレスに変換して（ステップＳ１１６）、リモートネームの取得を行ったBluetooth装置１０のアドレスとの比較を行う（ステップＳ１１７）。

【００７４】

アドレスが一致しない場合は、検査対象のBluetooth装置１０のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ１４に記録し、次のBluetooth装置１０のリモートネームを取得する。

【００７５】

ステップＳ１１７でアドレスが一致した場合は、２８文字目から残りの文字のサイズが３２文字かどうか検査し（ステップＳ１１８）、３２文字である場合は、認証用のデータとして取得し、取得した文字データを１６バイトのバイナリデータに変換する（ステップＳ１１９）。

【００７６】

サービス名称の長さ分のサービス名が取得できない場合、BTアドレス文字が６バイトのBluetoothアドレスに変換できない場合、残りの文字が３２文字と異なる場合、認証用データが数字に変換できない場合は、検査対象のBluetooth装置１０のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ１４に記録し、次のBluetooth装置１０のリモートネームを取得する。

【００７７】

ステップＳ１１９でバイナリデータに変換できた場合は、上記手順でリモートネームから取得したサービス名称と認証用データを用いて端末の認証を行う。

【００７８】

リモートネームを取得したBluetooth装置１０のBTアドレスを、「012345ABCDEF」の１２文字の文字データに変換する（ステップＳ１２０）。サービス名称文字とあわせた２２文字のデータは、１文字２バイトデータで表現されるため、全体で４４バイト、３５２ビットのサイズになる（ステップＳ１２１）。この３５

２ビットのデータに対してハッシュ演算を行い１２８ビットのハッシュ値を得る（ステップＳ１２２）。

【００７９】

取得した認証用データをあらかじめ準備された秘密鍵を用いて復号し、１２８ビットのハッシュ値を求める。この値と先ほど計算したハッシュ値を比較する（ステップＳ１２３）。相手が正しい秘密鍵を所持していれば、この値は一致し、一致したことを示すフラグを設定する（ステップＳ１２４）。秘密鍵が異なれば、復号化されたデータも異なるためハッシュ値は一致しない。一致しない場合は、検査中のBluetooth装置１０は、該当しないことを示すフラグをセットし（ステップＳ１２５）、次の装置のリモートネームを取得する。

【００８０】

悪意ある装置が、正しい装置に設定されたBluetooth装置１０の装置識別情報をコピーしても正しい装置と悪意ある装置のBluetoothアドレスが異なるため、ハッシュ値は一致しない。それゆえ、不正な装置を検出することが可能となる。

【００８１】

本実施形態では、双方共通の鍵を使用したが、公開鍵を使用しても同等の効果が得られる。Bluetooth装置１０の装置識別情報を作成するときは、秘密鍵を使用し、JAVAアプリケーションには秘密鍵に対応する公開鍵を含めて配布しても同等の効果が得られる。

【００８２】

上記実施形態では、Bluetooth装置１０の装置識別情報をあらかじめBluetooth装置１０に記録してあるが、Bluetooth装置１０が他の通信手段を有する場合は、その通信手段を通じて、定期的、あるいは、必要なときに、異なる秘密鍵で作成したBluetooth装置１０の装置識別情報を取得し、Bluetooth装置１０の装置識別情報を更新する。あわせて、JAVAアプリケーションも定期的にサーバにアクセスし、共通の秘密鍵を更新することにより、セキュリティを強化する方法も考えられる。あるいは、Bluetooth装置１０が秘密鍵をセキュアに保存できるのであれば、Bluetooth装置１０自身で、定期的に、あるいは、必要な時にBluetooth装置１０の装置識別情報を更新することができる。

【００８３】

また、ハッシュ値を作成する場合、双方秘密のデータを含めて作成することにより、セキュリティを強化する形態もありうる。

【００８４】

公開鍵を使用し、Bluetooth装置１０がBluetooth装置１０の装置識別情報を更新する場合は、Bluetooth装置１０のBTアドレスを含めず、時刻などの情報を変わりに用いることでも同等の効果が得られる。

【００８５】

あるいは、Bluetooth装置１０の装置識別情報に識別情報の有効期限を含めることにより、携帯端末はその有効期限を検査することにより、さらなるセキュリティの強化を行うことが可能となる。

【００８６】

また、OBEXなどの上位プロトコル接続のために、サービス情報取得プロトコルを実行して、接続に必要な情報の取得を行うが、あらかじめ、Bluetooth装置１０の装置識別情報に接続情報を含めることにより、サービス情報取得のための通信を省くことが可能となり、処理時間の短縮を行うことが可能となる。

【００８７】

Bluetooth携帯端末１１において、処理を早まるために、信頼できないと判定したBluetooth装置１０のアドレスを信頼できない装置のリストとしてメモリ１４に記録しておき、次回から、インクワイアリ終了後、発見したBluetooth装置１０のBTアドレスと、信頼できない装置のリストを比較し、その装置が信頼できないと判定した場合には、その装置を検査対象のリストに含めないことにより、全体の処理速度を向上させることが可能となる。

【００８８】

このように、本実施形態では、Bluetooth装置１０の装置識別情報を、サービス名称、BTアドレス及び暗号化データで構成するため、この装置識別情報を受け取ったBluetooth携帯端末１１は接続しようとするBluetooth装置１０が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性を向上できる。

【００８９】

上述した実施形態で説明した図４～図７の処理は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、図４～図７の処理を実行するプログラムをフロッピーディスクやＣＤ－ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【００９０】

また、図４～図７の処理を実行するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【００９１】

なお、本発明は、上記の実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。さらに、上記実施形態には種々の段階の発明は含まれており、開示される複数の構成用件における適宜な組み合わせにより、種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題（の少なくとも１つ）が解決でき、発明の効果の欄で述べられている効果（のなくとも１つ）が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００９２】

【発明の効果】

以上詳細に説明したように、本発明によれば、サービス名称と装置識別情報を含む第１識別情報を暗号化した暗号化データを生成し、サービス名称、装置識別情報及び暗号化データを含む第２識別情報を他の通信装置に送信するため、通信相手が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性能の向上が図れる。

【図面の簡単な説明】

【図１】

本発明に係る情報提供装置の一実施形態であるBluetooth装置１０の内部構成を示す図。

【図２】

Bluetooth携帯端末１１の内部構成の一例を示すブロック図。

【図３】

Bluetooth携帯端末１１の情報取得方法を示すフローチャート。

【図４】

サービス提供を行う前のBluetooth装置１０の準備作業を示すフローチャート。

【図５】

Bluetooth装置１０のサービス提供時の処理手順を示すフローチャート。

【図６】

Bluetooth携帯端末１１の処理手順を示すフローチャート。

【図７】

図６のステップＳ１００の検証手順の詳細フローチャート。

【図８】

Bluetooth端末が任意の場所で任意の相手からサービスを受けるための処理手順を示すフローチャート。

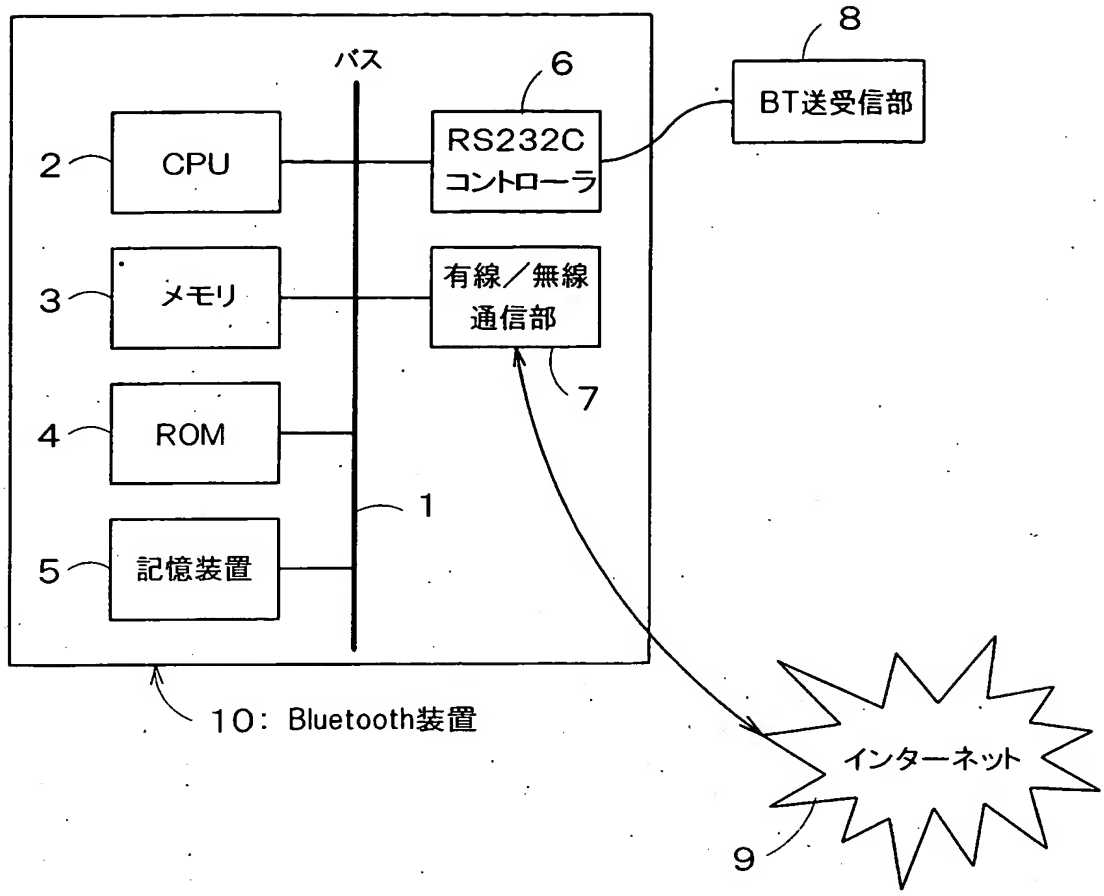
【符号の説明】

1　バス
2　CPU
3　メモリ
4　ROM
5　記憶装置
6　RS-232Cコントローラ
7　有線／無線通信部
8　BT送受信部
9　インターネット

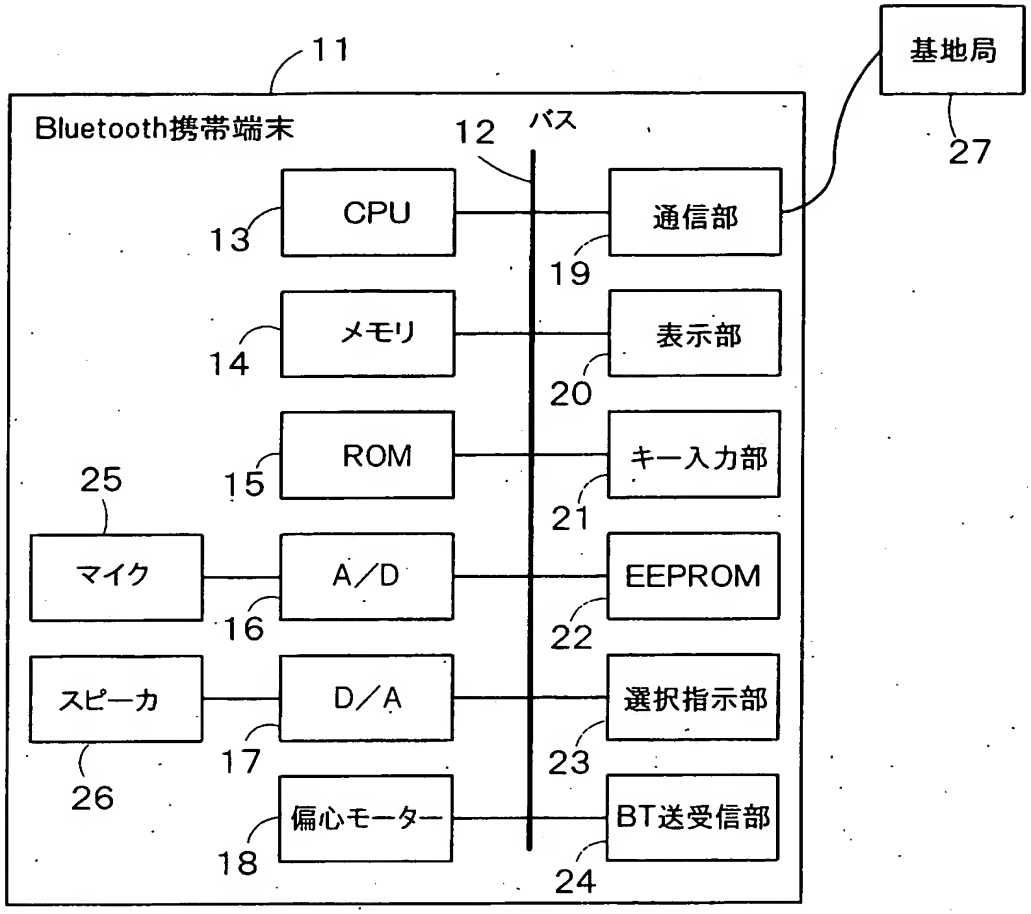
１０　Bluetooth装置
１１　Bluetooth端末
１２　バス
１３　CPU
１４　メモリ
１５　ROM
１６　A/D変換器
１７　D/A変換器
１８　偏心モータ
１９　有線／無線通信部
２０　表示部
２１　キー入力部
２２　EEPROM
２３　選択指示部
２４　BT送受信部
２５　マイク
２６　スピーカ
２７　基地局

【書類名】　図面

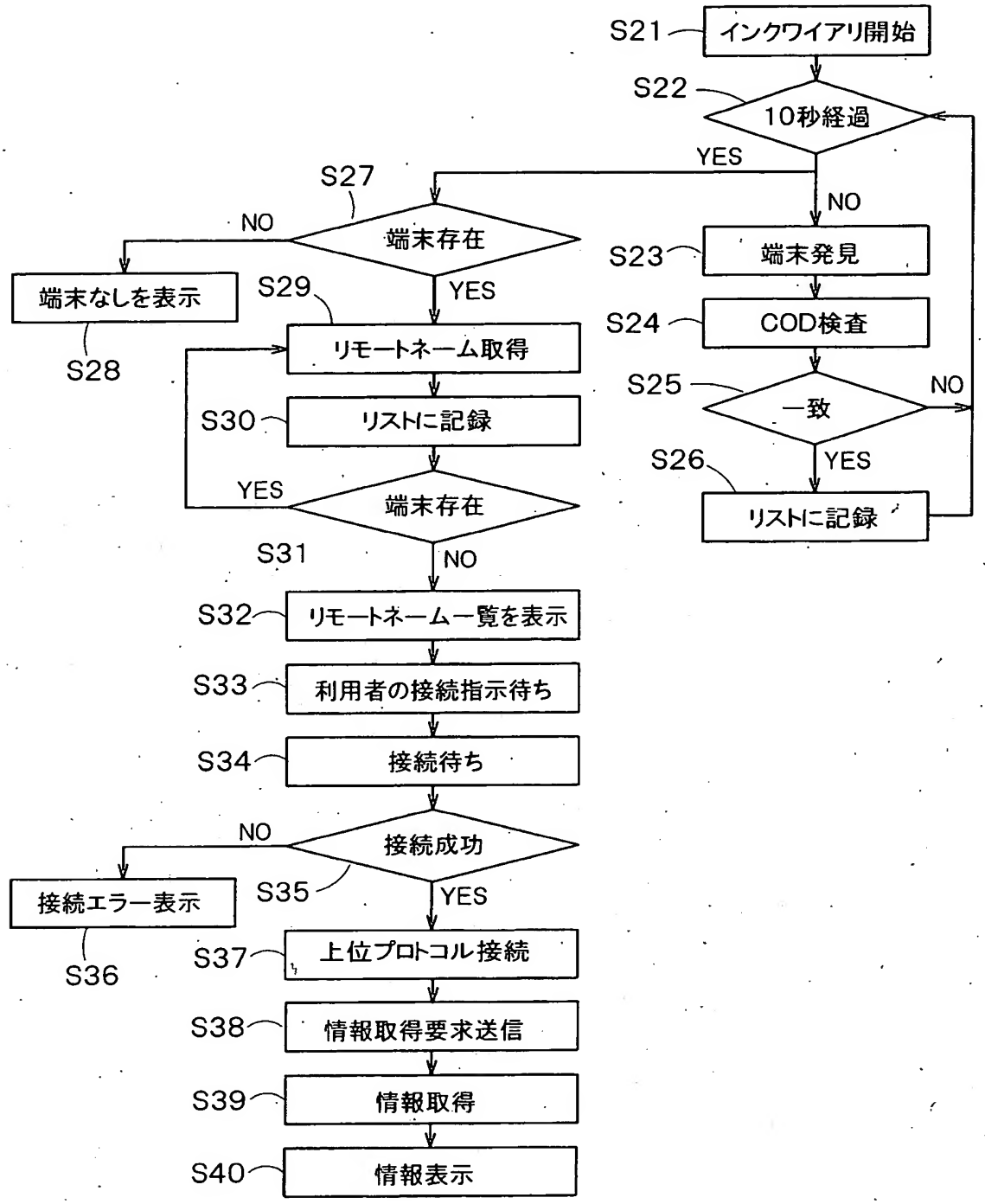
【図１】


バス
6
8
BT送受信部
2
CPU
RS232C
コントローラ
3
メモリ
有線／無線
通信部
7
4
ROM
1
5
記憶装置
10：Bluetooth装置
インターネット
9

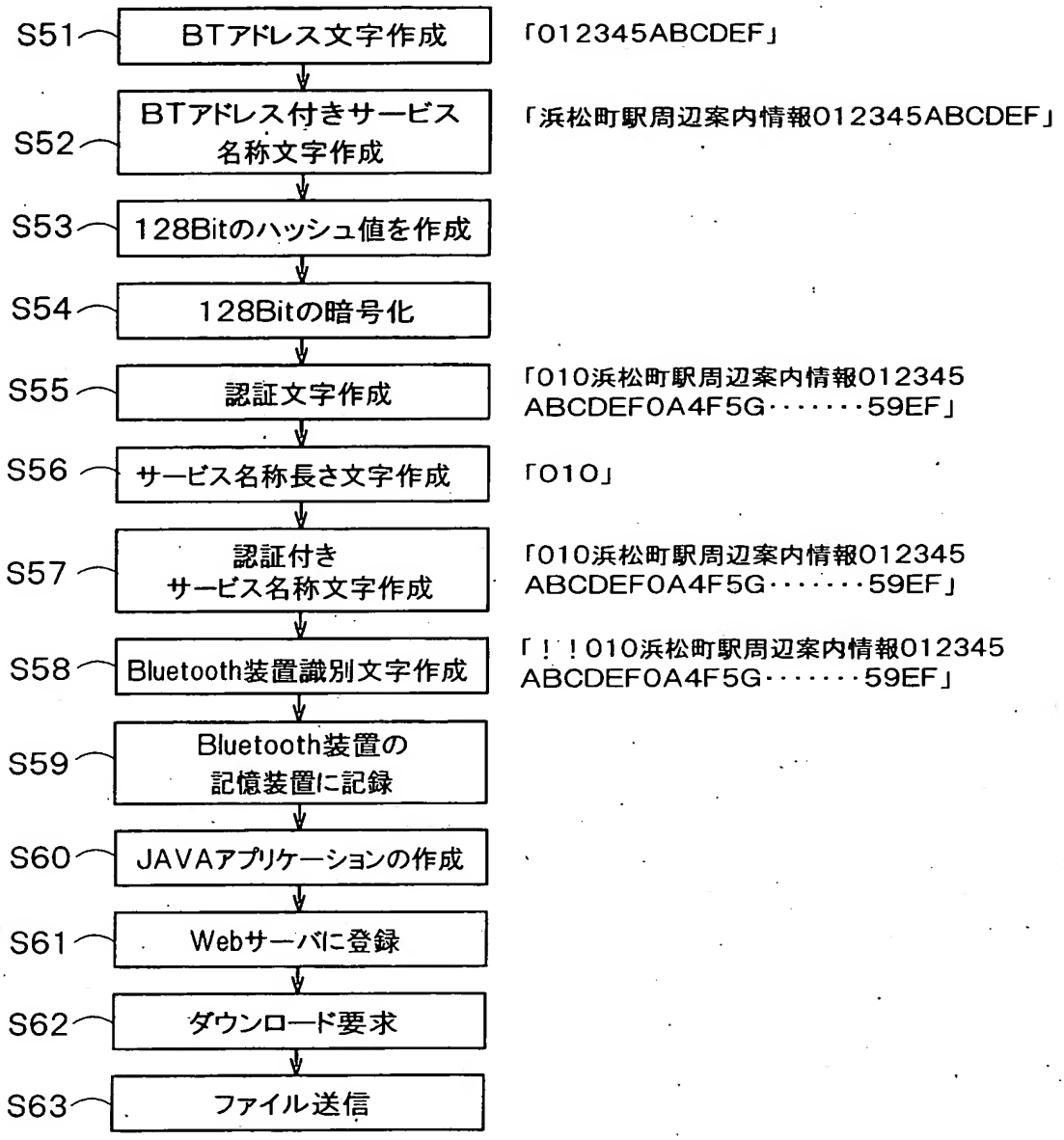
【図２】


11
Bluetooth携帯端末
12
バス
基地局
27
CPU
13
通信部
19
メモリ
14
表示部
20
ROM
15
キー入力部
21
25
マイク
A／D
16
EEPROM
22
スピーカ
D／A
17
選択指示部
23
26
偏心モーター
18
BT送受信部
24

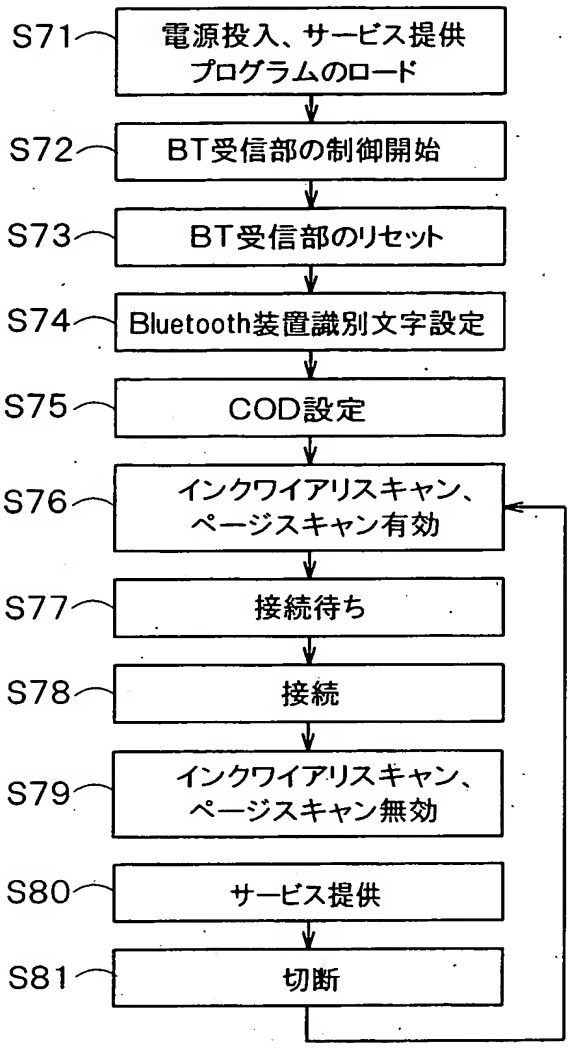
【図３】


S21
インクワイアリ開始
S22
10秒経過
YES
NO
S23
端末発見
S24
COD検査
S25
一致
NO
YES
S26
リストに記録
S27
端末存在
NO
YES
端末なしを表示
S28
S29
リモートネーム取得
S30
リストに記録
端末存在
YES
S31
NO
S32
リモートネーム一覧を表示
S33
利用者の接続指示待ち
S34
接続待ち
接続成功
NO
S35
YES
接続エラー表示
S36
S37
上位プロトコル接続
S38
情報取得要求送信
S39
情報取得
S40
情報表示

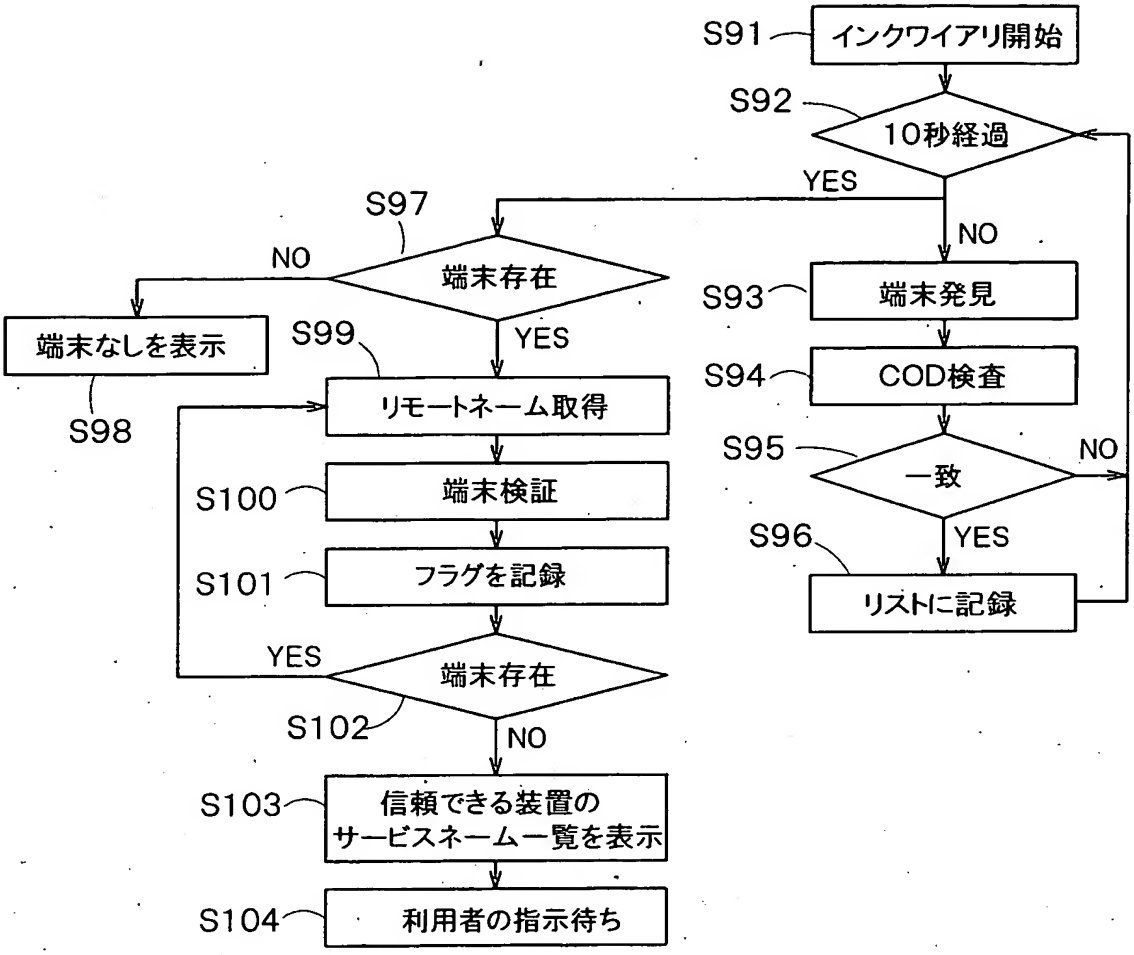
【図４】


S51
BTアドレス文字作成
「012345ABCDEF」
S52
BTアドレス付きサービス名称文字作成
「浜松町駅周辺案内情報012345ABCDEF」
S53
128Bitのハッシュ値を作成
S54
128Bitの暗号化
S55
認証文字作成
「010浜松町駅周辺案内情報012345 ABCDEF0A4F5G・・・・・・・59EF」
S56
サービス名称長さ文字作成
「010」
S57
認証付きサービス名称文字作成
「010浜松町駅周辺案内情報012345 ABCDEF0A4F5G・・・・・・・59EF」
S58
Bluetooth装置識別文字作成
「！！010浜松町駅周辺案内情報012345 ABCDEF0A4F5G・・・・・・・59EF」
S59
Bluetooth装置の記憶装置に記録
S60
JAVAアプリケーションの作成
S61
Webサーバに登録
S62
ダウンロード要求
S63
ファイル送信

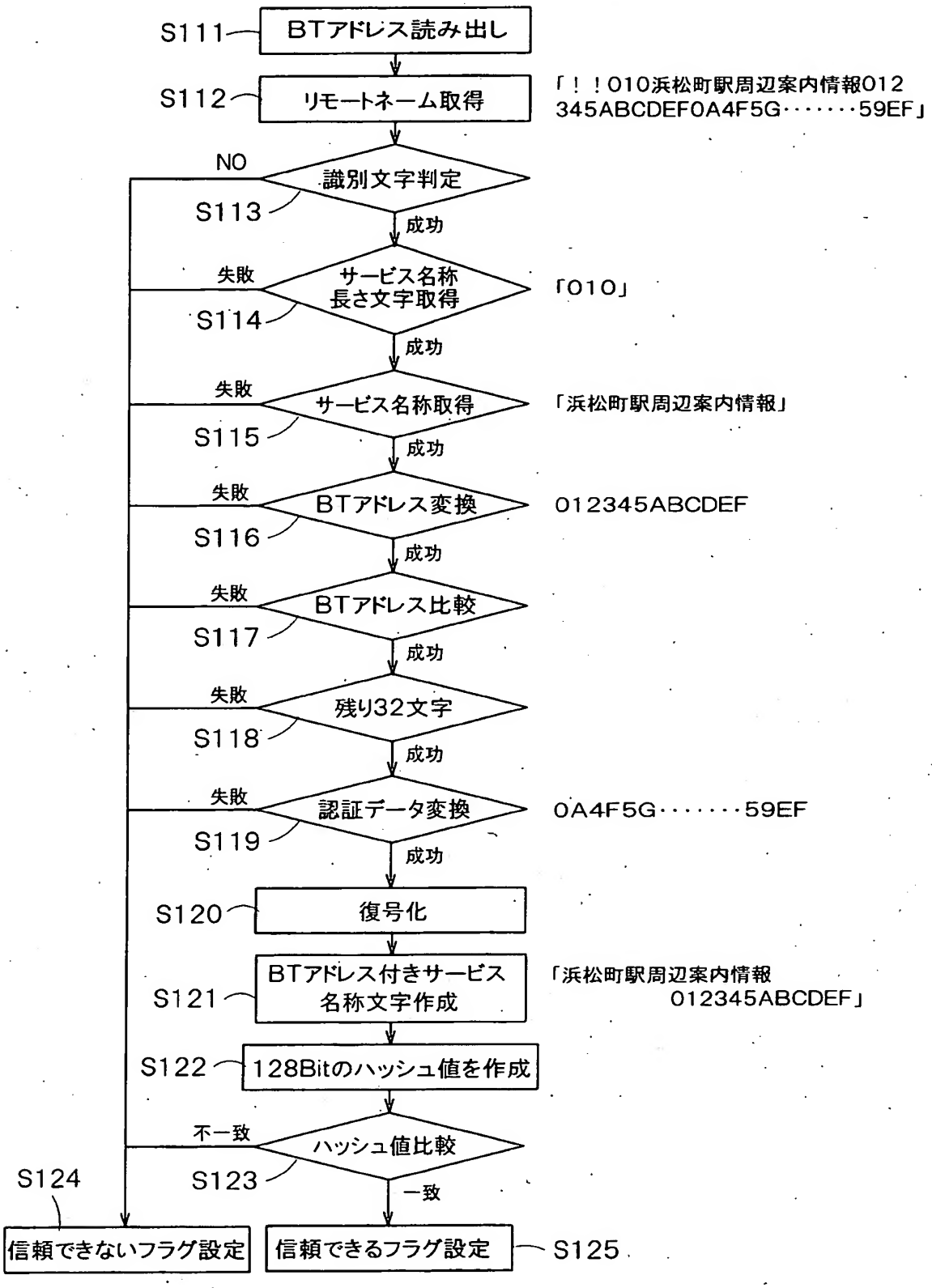
【図５】


S71
電源投入、サービス提供プログラムのロード
S72
BT受信部の制御開始
S73
BT受信部のリセット
S74
Bluetooth装置識別文字設定
S75
COD設定
S76
インクワイアリスキャン、ページスキャン有効
S77
接続待ち
S78
接続
S79
インクワイアリスキャン、ページスキャン無効
S80
サービス提供
S81
切断

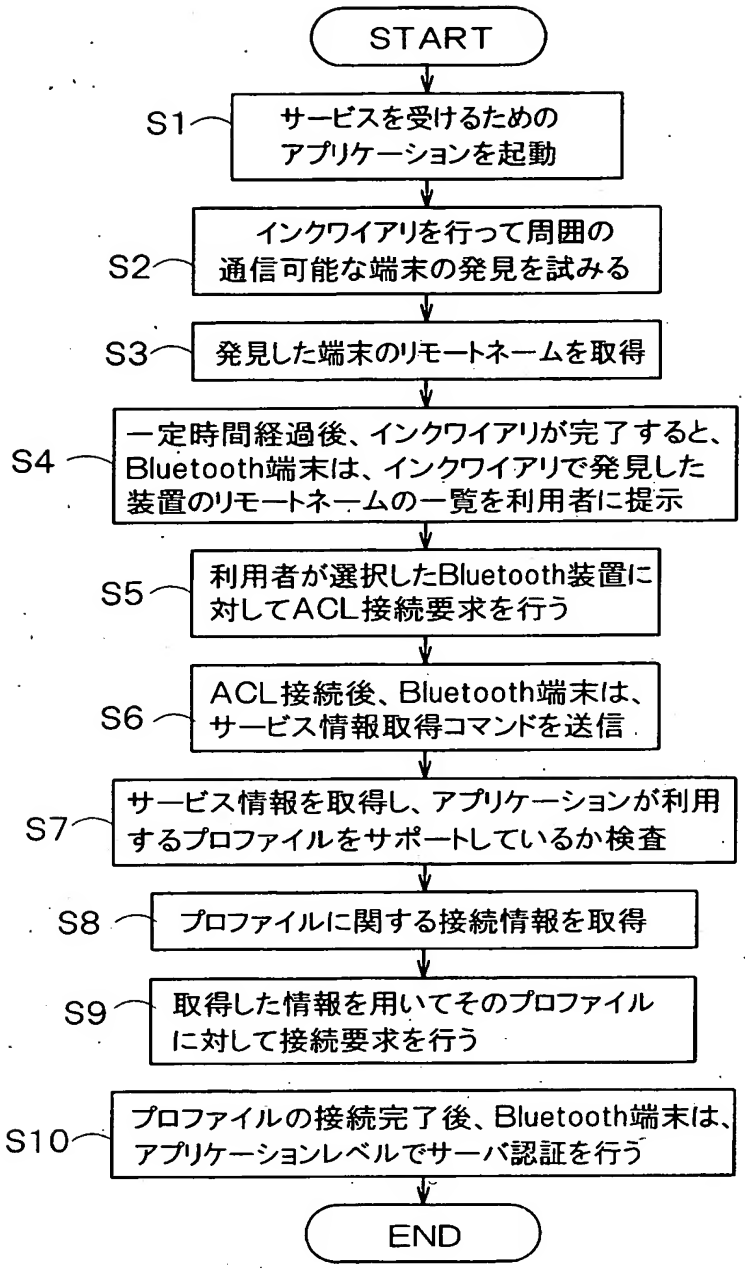
【図６】


S91
インクワイアリ開始
S92
10秒経過
YES
NO
S93
端末発見
S94
COD検査
S95
一致
NO
YES
S96
リストに記録
S97
端末存在
NO
YES
端末なしを表示
S98
S99
リモートネーム取得
S100
端末検証
S101
フラグを記録
S102
端末存在
YES
NO
S103
信頼できる装置の
サービスネーム一覧を表示
S104
利用者の指示待ち

【図７】


S111
BTアドレス読み出し
S112
リモートネーム取得
「！！010浜松町駅周辺案内情報012345ABCDEF0A4F5G・・・・・・・59EF」
NO
識別文字判定
S113
成功
失敗
サービス名称長さ文字取得
「010」
S114
成功
失敗
サービス名称取得
「浜松町駅周辺案内情報」
S115
成功
失敗
BTアドレス変換
012345ABCDEF
S116
成功
失敗
BTアドレス比較
S117
成功
失敗
残り32文字
S118
成功
失敗
認証データ変換
0A4F5G・・・・・・・59EF
S119
成功
S120
復号化
S121
BTアドレス付きサービス名称文字作成
「浜松町駅周辺案内情報012345ABCDEF」
S122
128Bitのハッシュ値を作成
不一致
ハッシュ値比較
S123
一致
S124
信頼できないフラグ設定
信頼できるフラグ設定
S125

【図８】


START
S1
サービスを受けるための
アプリケーションを起動
S2
インクワイアリを行って周囲の
通信可能な端末の発見を試みる
S3
発見した端末のリモートネームを取得
S4
一定時間経過後、インクワイアリが完了すると、
Bluetooth端末は、インクワイアリで発見した
装置のリモートネームの一覧を利用者に提示
S5
利用者が選択したBluetooth装置に
対してACL接続要求を行う
S6
ACL接続後、Bluetooth端末は、
サービス情報取得コマンドを送信
S7
サービス情報を取得し、アプリケーションが利用
するプロファイルをサポートしているか検査
S8
プロファイルに関する接続情報を取得
S9
取得した情報を用いてそのプロファイル
に対して接続要求を行う
S10
プロファイルの接続完了後、Bluetooth端末は、
アプリケーションレベルでサーバ認証を行う
END

【書類名】　　要約書

【要約】

【課題】　信頼できるサービスを提供する通信装置に簡易かつ迅速かつ正しく接続する。

【解決手段】　Bluetooth装置１０は、バス１に接続されたCPU２、メモリ３、ROM４、記憶装置５、RS-232Cコントローラ６及び有線／無線通信部７と、RS-232Cコントローラ６に接続されたBT送受信部８とを有する。Bluetooth携帯端末１１は、バス１２に接続されたCPU１３、メモリ１４、ROM１５、A/D変換器１６、D/A変換器１７、偏心モータ１８、通信部１９、表示部２０、キー入力部２１、EEPROM２２、選択指示部２３及びBT送受信部２４を有する。Bluetooth装置１０の装置識別情報を、サービス名称、BTアドレス及び暗号化データで構成するため、この装置識別情報を受け取ったBluetooth携帯端末１１は接続しようとするBluetooth装置１０が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性を向上できる。

【選択図】　図１

特願２００２－３２１３４８

出願人履歴情報

識別番号　［０００００３０７８］

１．変更年月日　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝

２．変更年月日　２００３年　５月　９日
［変更理由］　名称変更
住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝